UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,937	08/20/2001	Masahiro Kaminaga	NITT.0027	4651

38327 7590 11/19/2004

REED SMITH LLP
3110 FAIRVIEW PARK DRIVE, SUITE 1400
FALLS CHURCH, VA 22042

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,937	KAMINAGA ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-12 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-12 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 20 August 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 8/20/01, 7/14/03.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12 have been examined.

Specification

2. The abstract of the disclosure is objected to because it contains more than one paragraph and exceeds 150 words in length. Correction is required. See MPEP § 608.01(b).

Claim Objections

3. Claims 7 and 11 are objected to because of the following informalities: "encryption processing method" in the first line of each claim should be changed to "decryption processing method". Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Regarding claims 1, 5 and 9, the claims recite the limitation "suppressing the output of said processing result" in clause (4) of each claim. There are two processing results, Z and W, and it's not clear which processing result is

referred to by the limitation. For examination purpose, the limitation is interpreted as "suppressing the output of said processing result Z" in each claim. Claims that are not specifically addressed are rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by Blanchard et al. (6,219,791). Blanchard discloses a method comprising the steps of:

performing an encryption process in which a secret key K is to be applied to an input plaintext M, and storing a processing result Z in a memory (fig. 4, step 420; fig. 1, elements 12, 20 and 30);

performing a decryption process for said processing result Z on said memory and storing the decryption result W on the memory (fig. 4, step 430; fig. 1, element 30);

outputting said processing result Z when said processing result W coincides with said plaintext M (fig. 4, step 470); and

suppressing the output of said processing result Z when said processing result W does not coincide result when with said plaintext M (fig. 4, step 480).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blanchard as applied to claim 1 above, and further in view of Fernandez-Gomez et al. ("Concurrent Error Detection in Block Ciphers"). Daniels does not disclose using DES algorithm. Fernandez-Gomez discloses using DES algorithm (p. 980, right col., "The technique proposed ... in section 4"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Daniels method to use DES algorithm, as taught by Fernandez-Gomez. The motivation for doing so would have been that DES is a current and widely used encryption algorithm.

10. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blanchard as applied to claim 1 above, and further in view of Ogg et al. (US 2002/0178354 A1). Daniels does not disclose that the device is reset. Ogg discloses a cryptographic device being reset (par. 0042). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Daniels method such that the

device is reset, as taught by Ogg. The motivation for doing so would have been to protect against attempts to retrieve critical information.

11. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blanchard as applied to claim 1 above, and further in view of Boneth et al. ("On the Importance of Checking Cryptographic Protocols for Faults"). Daniels does not disclose an IC card performing the method of claim 1 to verify a cryptographic process. Boneth discloses a smart card verifying the correctness a cryptographic computation (p. 38, 4th par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Daniels method such that it is implemented on a smart card, as taught by Boneth. A smart card needs to verify the correctness a cryptographic computation to prevent the danger that hardware faults poses to various cryptographic protocols.

12. Claim 5-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daniels et al. (5,991,401) in view of Fernandez-Gomez. Daniels discloses a method comprising the steps of:

performing a decryption process wherein a master key is to be applied to an input ciphertext C, and storing a processing result Z in a memory (fig. 3, step 41);

performing an encryption process for said processing result Z on said memory using an encryption key, and storing the result W on the memory (fig. 3, step 42);

outputting said processing result Z when said processing result W coincides with said ciphertext C (fig. 3, step 44); and

suppressing the output of said processing result Z when said processing result W does not coincide result when with said ciphertext C (fig. 3, step 45).

Daniels does not disclose using a symmetric algorithm. Fernandez-Gomez discloses using DES, which is a symmetric algorithm (p. 980, right col., "The technique proposed ... in section 4"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Daniels method to use DES algorithm, as taught by Fernandez-Gomez. The motivation for doing so would have been that DES is a current and widely used encryption algorithm. Accordingly, the same key is used in both encryption and decryption processes.

13. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniels in view of Fernandez-Gomez as applied to claim 5 above, and further in view of Ogg. Daniels and Fernandez-Gomez do not disclose that the device is reset. Ogg discloses a cryptographic device being reset (par. 0042). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Daniels and Fernandez-Gomez such that the device is reset, as taught by Ogg. The motivation for doing so would have been to protect against attempts to retrieve critical information.

14. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniels in view of Fernandez-Gomez as applied to claim 5 above, and further in view of Boneth. Daniels and Fernandez-Gomez do not disclose an IC card performing the method of claim 1 to verify a cryptographic process. Boneth discloses a smart card verifying the correctness a cryptographic computation (p. 38, 4th par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Daniels and Fernandez-Gomez such that it is implemented on a smart card, as taught by Boneth. A smart card needs to verify the correctness a cryptographic computation to prevent the danger that hardware faults poses to various cryptographic protocols.

15. Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daniels et al. (5,991,401) in view of Schneier ("Applied Cryptography"). Daniels discloses a method comprising the steps of:

performing a decryption process wherein the decryption key of a decryption-encryption key pair, which meets the limitation of a private key, is to be applied to an input ciphertext C, and storing a processing result Z in a memory (fig. 3, step 41);

performing an encryption process for said processing result Z on said memory using the encryption key of the key pair, which meets the limitation of a public key, and storing the result W on the memory (fig. 3, step 42);

outputting said processing result Z when said processing result W coincides with said ciphertext C (fig. 3, step 44); and

suppressing the output of said processing result Z when said processing result W does not coincide result when with said ciphertext C (fig. 3, step 45).

Daniels does not disclose using the RSA algorithm. Schneier discloses using RSA algorithm (Section 19.3, p. 466-467, "Soon after Merkle's knapsack ... confidence level in the algorithm"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Daniels method to use RSA algorithm, as taught by Schneier. The motivation for doing so would have been that RSA is the easiest to understand and implement of all public-key algorithms. Accordingly, the same key is used in both encryption and decryption processes.

16. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniels in view of Schneier as applied to claim 9 above, and further in view of Ogg. Daniels and Schneier do not disclose that the device is reset. Ogg discloses a cryptographic device being reset (par. 0042). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Daniels and Schneier such that the device is reset, as taught by Ogg. The motivation for doing so would have been to protect against attempts to retrieve critical information.

17. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniels in view of Schneier as applied to claim 9 above, and further in view of Boneth. Daniels and Schneier do not disclose an IC card performing the method of claim 1 to verify a cryptographic process. Boneth discloses a smart card verifying the correctness a

cryptographic computation (p. 38, 4th par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Daniels and Schneier such that it is implemented on a smart card, as taught by Boneth. A smart card needs to verify the correctness a cryptographic computation to prevent the danger that hardware faults poses to various cryptographic protocols.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Likens et al. (5,608,798) discloses a cryptographic device with secure testing function.

Laih et al. (6,144,740) discloses a method for designing public key cryptosystems against fault-based attacks.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
11/09/04

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100